Software Engineering Institute
Carnegie Mellon University

Intelligence Preparation for Operational Resilience (IPOR)

Douglas Gray

December, 2015

SPECIAL REPORT
CMU/SEI-2015-SR-033

CERT Program

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0002686

Table of Contents

List of Figures

List of Tables

Acknowledgments

The support of Tim Casey of Intel Corporation and Jim Lippard of American Express was critical to understanding both the private sector's perspective on intelligence and the processes that organizations such as Intel are using to operationalize intelligence analysis. Throughout the process, Jay McAllister of the Software Engineering Institute's Emerging Technology Center readily provided his deep insights into the needs and trends he has seen in cyber threat intelligence, as well as connecting me to other subject-matter experts in the industry. I would also like to thank Sidney Faber, Pamela Curtis, and Laurie Tyzenhaus of the Software Engineering Institute for providing their input in the development of this report. Finally, the support of my division and team leadership, Summer Fowler and Brendan Fitzpatrick, was instrumental in enabling the development of this framework.

Abstract

Operational resilience practitioners in industry, government, and the military have the unenviable task of recommending and acting upon priorities to enable their organizations to accomplish their missions during times of stress. However, for many, a formal method of acquiring and leveraging objective threat intelligence to support resilience, risk, and project management has remained elusive. This special report proposes a framework called Intelligence Preparation for Operational Resilience (IPOR) to create a model for structured analysis of their intelligence needs and a way to operationalize threat intelligence once they have received it. The IPOR references and builds upon frameworks such as the military's Intelligence Preparation of the Battlefield process and the CERT® Resilience Management Model to build a structure to meet this end.

1 Introduction

> *If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.*
>
> *Sun Tzu*[1]

The quintessential difference between operational resilience and other information technology (IT) disciplines, such as software development and IT operations, is the existence of a threat actor. In planning and managing operational resilience, the intentions, capabilities, and prevailing attack patterns of threat actors form the basis for determining which actions take priority while balancing the organization's services, reputation, and bottom line. However, how do operational resilience practitioners take the diverse (and sometimes conflicting) streams of threat intelligence and inject them into established frameworks for resilience, risk, and project management? How do they make use of intelligence to support operational resilience?

Existing frameworks for resilience, risk, and project management contain numerous touchpoints at which intelligence needs can be identified and products consumed in a structured, pragmatic way, without giving in to the dreaded triad of fear, uncertainty, and doubt. The United States military does this continuously as part of its Military Decision-Making Process (MDMP) and Intelligence Preparation of the Battlefield (IPB) process [ADP 5-0, p. 8]. While originally designed to support kinetic military operations, MDMP and IPB have both become staples in cyber-related planning in the military and can be adapted to management techniques in civilian spheres. Adapting IPB to common resilience, risk, and project-management frameworks can provide a powerful source of requirements and quality attributes for operational resilience functions for civilian organizations.

To accomplish this goal, this report describes Intelligence Preparation for Operational Resilience (IPOR), a complementary framework for preparing intelligence. IPOR is intended to be used during operational resilience planning to provide context to risk management decisions. It extends IPB to the cyber mission in civilian organizations by placing it in a context relevant to civilian operational resilience practitioners.

Just as civilian and IT planning processes include a phase that assesses stakeholder needs and determines requirements for the portfolio, program, or project, the MDMP contains a set of tasks called Mission Analysis. It identifies facts, assumptions, risks, and constraints as well as tasks both specified or implied by higher headquarters. Part of this process is identifying and consuming required intelligence as part of the IPB process. IPB assesses the organization's mission and identifies the organization's needs for intelligence collection. It then determines how the organization will consume those intelligence products to include key decision points for commanders [U.S. Army 2014, p. 1]. While the organization must maintain situational awareness of its own

[1] http://classics.mit.edu/Tzu/artwar.html.

posture when considering operational resilience, it must also frame identified existing vulnerabilities by considering threats and threat actors [Caralli & Allen 2010, pp. 923-924].

The IPOR model references and builds upon IPB to develop a threat-analysis framework that all organizations can use for operational resilience. IPB is a time-tested process for supporting adversarial operations. The U.S. military has used it for decades in a wide variety of operations, including major combat operations, force protection, peacekeeping, and defensive and offensive cyber operations. It is also adaptable to situations with both abundant and constrained time for analysis. However, it has two limitations for our purposes. First, the terminology is decidedly military and may not be accessible to those without a military planning background. Second, there is an opportunity for a deeper treatment of operational resilience considerations.[2] A full analysis of the IPB process is outside the scope of this document.

1.1 Threat Actors, Threats, and Risks

Threat actors come in a variety of forms. The CERT® Resilience Management Model (CERT-RMM) defines a threat actor as "a situation, entity, individual, group, or action that has the potential to exploit a threat." CERT-RMM further defines a threat as "the combination of a vulnerability, a threat actor, a motive (if the threat actor is a person or persons), and the potential to produce a harmful outcome for the organization." Threats can come from physical sources such as weather (e.g., floods and earthquakes) and human hazards to facilities (e.g., terrorist attacks and civil unrest). They can also be the logical threats we normally associate with cybersecurity (e.g., activity by nation states, criminal elements, hacktivists, cyber-terrorists, and insider threats).

According to CERT-RMM, "Risk is the combination of a threat and a vulnerability (condition), the impact (consequence) on the organization if the vulnerability is exploited, and the presence of uncertainty. In CERT-RMM, this definition is typically applied to the asset or service level such that risk is the possibility of suffering harm or loss due to disruption of high-value assets and services."

IT professionals must consider quality attributes such as performance, reliability, and modifiability based on stakeholder requirements [Clements 2011, Kindle locations 767, 789-801]. Just as market research may drive the quality attributes of a system from the user's perspective, the intentions, capabilities, and prevailing attack patterns of a threat actor form the basis of security-related requirements and quality attributes of a system and the organizations it supports. A realistic, objective, and practical awareness of current threat actor characteristics and the environment in which threat actors and the defending organization operate are essential to planning for operational resilience.

1.2 Operational Resilience

CERT-RMM defines operational resilience as "the ability of the organization to achieve its mission even under degraded circumstances." Physical and logical threat actors cause these degraded circumstances. Mission success starts with operational risk management, which depends upon effectively analyzing threat actors. Because threat actors continually evolve, an organization must

[2] Army Techniques Publication 2-01.3 provides the background and process for IPB and can be accessed by the public at http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/atp2_01x3.pdf.

continuously review and refine its operational resilience program through discipline and a common understanding of process [Caralli & Allen 2010, pp. 1-5]. In other words, *what* an organization does to optimize resilience rarely changes. *How* an organization meets its resilience needs is constantly evolving.

1.3 The Role of IPOR

This special report focuses on how an organization identifies its intelligence collection and analysis needs and integrates collected intelligence into its resilience, risk, and project-management frameworks. Often, the results of intelligence collection will lead not to an actionable decision, but rather to additional or refined intelligence collection. This document discusses how an organization can more effectively interface with intelligence-collection personnel (whether in-house or outsourced) and make its own decisions about the priorities and mitigations of risks identified or clarified through the process. Although this report briefly touches upon intelligence collection and analysis, that is not its focus. Where intelligence collection is discussed, it is only to provide context to the process of integrating intelligence products into the frameworks discussed in Section 1.4 below. That is, the operational resilience practitioner must analyze the analysis he or she receives and determine the meaning (or "so what") for the organization [U.S. Army 2014, p. 3-2]. Although this report discusses stakeholder considerations in determining intelligence needs, it does not seek to proscribe formats and methods of delivering intelligence products. Instead, it sets up an intellectual framework for organizing intelligence needs and means to enable effective operational resilience decisions and actions.

1.4 Considerations for Use of IPOR

1.4.1 Building Threat Intelligence into Operational Resilience Planning

Operational resilience practitioners must develop a routine, collaborative, trust-based relationship with the intelligence analysts who develop threat intelligence for them. Intelligence analysts need to understand how operational resilience practitioners think and prioritize intelligence. Resilience practitioners must come to trust intelligence products and provide feedback to intelligence analysts [Gray 2015].

1.4.2 Making Intelligence Actionable

Operational resilience is the result of a series of Observe, Orient, Decide, Act (OODA) loops, a concept first conceived by Air Force Col. John Boyd. Members of the organization perceive the situation around them using their five senses, make sense of that output, make decisions regarding that orientation, and then act upon the decision. While generally sequential, as Figure 1 shows, the OODA loop provides feedback from step to step (e.g., orientation implicitly guided and controls observation) that enable a more fine-tuned process. An effective and efficient OODA loop enables people and organizations to maximize their understanding of a situation. They can then effect solutions based on the best available information and analysis and with improved timeliness [Boyd 1996].

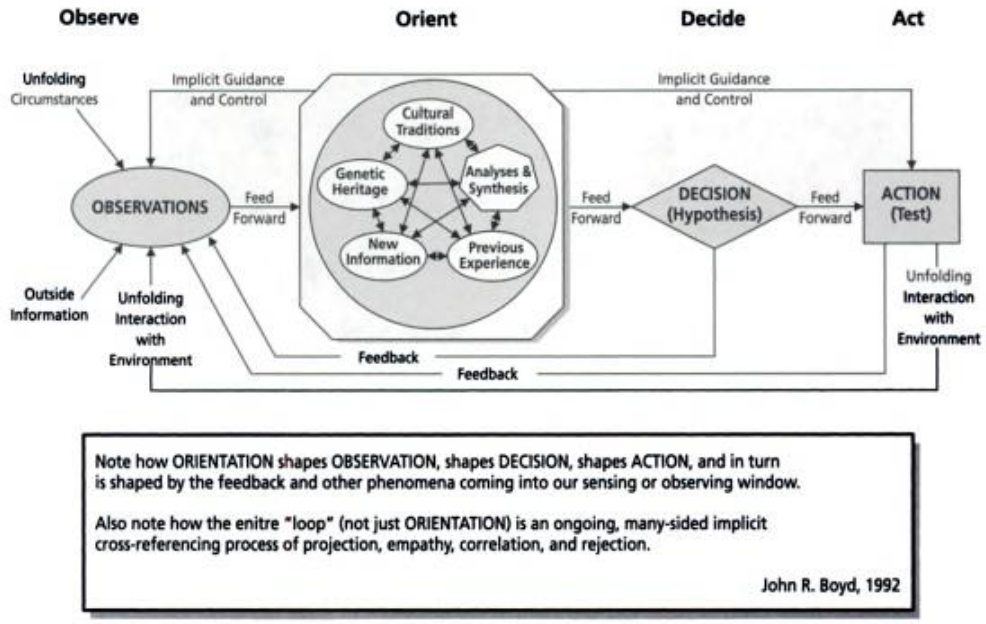

Figure 1: The OODA Loop [Boyd 1996]

1.4.3 Organizing Input and Analysis Steps

To attain more effective situational awareness, an operational resilience practitioner needs to break down (or decompose) information in order to make decisions and take actions. Situational awareness is defined as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status into the near future" [Endsley 2012, p. 13]. This situational awareness takes place at three distinct levels:

- Level 1—perception of the elements in the environment
- Level 2—comprehension of the current situation
- Level 3—projection of future status [Endsley 2012, p. 14]

Without decomposing information at these three levels, it is easy to become overwhelmed and fail to grasp the importance, validity, and relevance of information. Decomposing the problem into smaller pieces makes the entire process more formal and repeatable, leading to greater maturity. Each category has an effect upon (or a "voice") in the decisions and actions to be made. One method is to decompose sources of situational awareness into three voices:

1. **Voice of the Environment** includes technical trends, socio-political trends, and legal contexts. (This is discussed in Section 2.1.)
2. **Voice of the Organization** centers on the organization and its supporting assets and services. (This is discussed in Section 2.2.) It decomposes into two sub-categories.
    a. **Voice of the Mission** includes the organization's circle of influence, its strategic vision and objectives, and organizational culture.
    b. **Voice of the Service** includes the organization's risk profile, operational profile, and resources.

3. **Voice of the Threat Actor** includes information such as a threat's physical and logical personae (if available), threat categorizations, motivations, capabilities, and prevailing attack patterns (i.e., their methods for exploiting assets and services) [Barnum & Sethi 2007, p. 1]. (This is discussed in Section 2.3.)

Of the three voices, the Voice of the Organization falls into what Stephen Covey called an organization's "circle of influence," or considerations that the organization can affect, such as spending, hiring, purchasing and training. The other two—the Voice of the Threat Actor and the Voice of the Environment—fall into what Covey terms the organization's "circle of concern," considerations that may affect the organization but which the organization does not directly affect. Actions taken within the organization's circle of influence can compensate for considerations in the organization's circle of concern [Covey 2013, pp 81-88].

1.4.4 Framing Cyber Intelligence for Practical Use

When consuming intelligence products and communicating their contents to key stakeholders, it is important to identify how different stakeholders will make decisions, and therefore consume the information. "Stakeholdering" the information gives the resulting products more impact. For instance, executives consider information based on their mission and the constituencies to whom they have to answer. If they changed jobs, they would consider information differently according to their new mission and constituencies [Allison & Zelikow 1999, Kindle location 5603]. Intelligence products are received more readily when they satisfy the questions that an executive stakeholder must answer to his or her constituencies in support of his or her mission.

Those in more execution-oriented roles will need information to successfully carry out the standard procedures that they must follow [Allison & Zelikow 1999, Kindle location 3235]. Understanding these standard procedures and communicating intelligence within that context helps these stakeholders to make more effective and immediate use of information.

Appendix A contains a more in-depth discussion of assessing stakeholder needs according to behavioral models. Applying the presentation of intelligence products to the model by which a stakeholder functions enables the stakeholder to more readily comprehend information.

1.4.5 Identifying and Compensating for Common Distortions in Intelligence Analysis

When you are attempting to understand the OODA Loop of a threat actor or categories of threat actors, ambiguities can distort the facts, assumptions, and importance of related intelligence. Many misperceptions are based in our psychology as human beings [Heuer 1999, pp. 115-146]. The same psychological distortions that can cause an intelligence analyst to misinterpret intelligence inputs can also cause those who rely on this intelligence to misinterpret it. Understanding these distortions and comparing them to the intelligence received helps the resilience practitioner to avoid them. It also enables the resilience practitioner to spot when the analysis may have fallen victim to them. When engaged productively, this can lead to a more productive relationship with intelligence analysts, ensuring that the organization's resilience needs are met with respect to cyber intelligence. Appendix B provides a more in-depth discussion of these distortions.

1.4.6 Operationalizing Threat Intelligence

IPOR also extends IPB by introducing touchpoints with the following resilience, risk, and project-management operational frameworks:

- CERT-RMM
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro
- National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)
- Agile
- Project Management Body of Knowledge (PMBOK)

Many organizations in the public and private sector use one or more of these frameworks for their information technology and other programs affecting operational resilience. Each framework can be used individually or in combination. By seamlessly integrating their intelligence analysis processes with these frameworks, organizations can achieve awareness, agility, and effectiveness. Using these frameworks to leverage threat intelligence is discussed in greater detail in Section 3.

2 Intelligence Preparation for Operational Resilience (IPOR)

The IPOR model identifies threat-related factors in the context of environmental and organizational factors that should be considered in resilience, risk, and project management. This framework is not intended to be used as a sequential checklist, as these factors can be affected by rapidly changing information. Rather, operational resilience practitioners should capture what information they can when they can and update it as new information becomes available. Otherwise, the process tends to halt due to incomplete information.

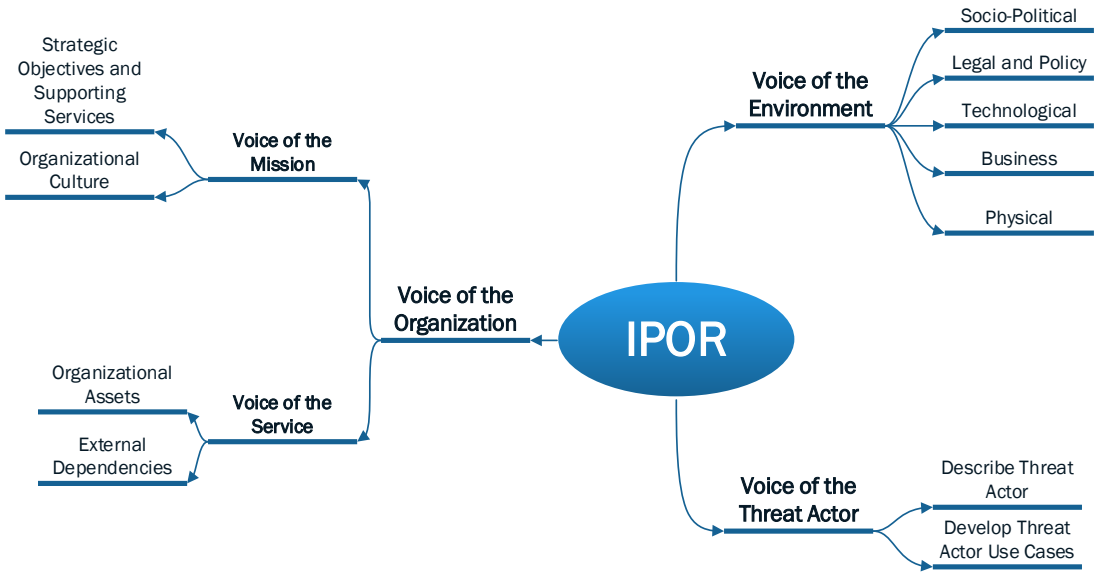

Figure 2: Intelligence Preparation for Operational Resilience Overview

The components of the IPOR are presented as considerations for analysis. The degree of formality in analyzing and documenting these considerations is directly affected by the time and resources available. An incomplete analysis is better than no analysis at all, since these considerations can be revisited and routinely updated either according to a routine schedule, or as facts and assumptions change. Even documenting incorrect analysis is important, as it gives the organization an understanding of the historical thought process that went into a previous resilience, risk, or project management decision. The organization should document and update these considerations both with regards to the threat actor's potential intentions, capabilities, and prevailing attack patterns and the potential risk to the organization's high-value assets and services.

The Voice-of-the-Organization section of the IPOR relies extensively on CERT-RMM process areas and specific goals and practices. However, this model is not presented as a capability maturity model. That said, this framework could ultimately be adapted into a model that assesses and evaluates the considerations within these three voices as specific goals and practices. Institutional-

ization of the organization's IPOR process could be assessed using the generic goals and practices outlined in CERT-RMM.[3]

2.1 Determine the Voice of the Environment

The Voice of the Environment is a set of considerations that may affect the organization's assets and services, as well as the threat actor's intentions, capabilities, and prevailing attack patterns. It provides the context for assessing the Voice of the Organization (discussed in Section 2.2) and the Voice of the Threat Actor (discussed in Section 2.3).

2.1.1 Determine the Socio-Political Environment

Organizations should identify socio-political events and trends that affect the threat actor's intentions, capabilities, and prevailing attack patterns. This in turn affects the organization's risk profile. Because network-based threats do not adhere to national boundaries, political events that are not associated with the organization can still affect it. For instance, several recent nation-state conflicts included a cyber component that employed botnets to attack the intended target. The latent presence of malware on an organization's network can cause the organization to become an unwitting participant in an attack. Various socio-political trends could also affect the perceived standing of the organization, attracting hacktivists who seek to make a political point by activities such as exfiltrating and posting data or defacing the organization's web presence. (Posting customer data from the Ashley Madison service is an example of such activity.) Finally, changes in the political relationships between nation states could either improve or degrade cybersecurity cooperation, which could affect the behavior of threat actors.

2.1.2 Determine the Legal and Policy Environment

Statutes such as the Health Insurance Portability and Accountability (HIPAA) Act, Sarbanes-Oxley (SOX) Act, Gramm-Leach-Bliley Act (GLBA), Federal Information Security Modernization Act (FISMA), and bills under consideration affect an organization's ability to share situational awareness data. They also affect how a compromise of operational resilience impacts the organization. The Computer Fraud and Abuse Act criminalizes the use of a protected computer to obtain information without authorization or to exceed one's authorized access level [Rustad 2009, Kindle location 3175]. The Electronic Communications and Privacy Act (ECPA)[4] and Section II of the ECPA, titled the Stored Communications Act[5], establish rights and restrictions on those who can access data in transit or at rest [Rustad 2009, Kindle location 3293]. In addition, laws (and subsequent case law) affect whether an insider is considered to be a threat actor. For instance, the law holds that the copyright of intellectual property (IP) developed as a "work for hire" belongs to the rights holder, not the creator of the IP who is hired to perform the work [Rustad 2009, Kindle location 3766]. In this case, a developer of company IP who takes this material to a subsequent position is considered to be a threat actor.[6] Additionally, court cases may change both

---

[3] More information on CERT-RMM can be found at http://www.cert.org/resilience/products-services/cert-rmm/.

[4] The text of the ECPA can be found at https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119.

[5] The text of the SCA can be found at https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121.

[6] Additional information on insider threats can be found at http://www.cert.org/insider-threat/.

the legal liability of the organization and the ways in which statutes are enforced. For example, courts often rule that statutes are unenforceable even though they remain on the books. Likewise, the penalties meted out in criminal and civil cases can radically change the potential impact of risks.

Many companies transfer some of their risks through insurance. However, changes in insurance coverage or organizational policy with regards to breach response (i.e., loss reimbursement or paid credit reporting) also change how a threat affects the organization's overall risk profile.

Finally, changes in statutes, treaties, and law enforcement also affect the recourse a compromised organization has in pursuing threat actors. This in turn affects the threat actor's behavior and the organization's risk profile. For instance, if a nation that was considered a safe haven for threat actors signed an extradition treaty with the organization's host nation, threat actors might be less willing to commit cybercrimes.

This section serves only as an introduction to the idea of assessing the legal and policy environment. Because of the rapid change and nuances in the legal environment, the operational resilience practitioner should cultivate a relationship of routine consultation with qualified legal counsel regarding the latest state of jurisprudence.

2.1.3 Determine the Technological Environment

Changes in the technical landscape can also affect the patterns of attacks by threat actors. For instance, threat actors may stage attacks that take advantage of the scalable, on-demand capacity of cloud services even if the organization does not use these services. What's more, ever-evolving mobile technologies make the organization's perimeter increasingly diffused. Threat actors could employ mobile technology to access organizational assets and services through remote connections. They could also compromise the physical possession of mobile devices such as phones and laptops. Changes in encryption capabilities also affect the threat actor's capabilities. An example would be the compromise of an encryption technology that the organization relied upon for data access or authentication. As computing power increases, the organization may find that an authentication regimen that once served it well is becoming less and less sufficient, which enhances the capabilities of threat actors.

2.1.4 Determine the Business Environment

A breach may have immediate, monetizable effects on an organization, such as the cost of paying for credit reporting. However, its impact is exacerbated by additional effects such as loss of consumer and shareholder confidence or reduced ability to perform its mission. An organization should consider that threat actors may attack the organization's services in order to damage the organization's stakeholders. Another consideration is how operational resilience influences the brand image of similar organizations in the market segment. If customers value the security of assets and services highly when making purchasing decisions, this could affect the organization's risk profile.

2.1.5 Determine the Physical Environment

Finally, the organization should not discount the role that physical factors play in operational resilience. For instance, if the distance between primary and alternate computing sites is insuffi-

cient, the organization may be at increased risk from natural threats such as major storms or seismic activity. Proximity to areas such as tectonic fault lines and areas prone to tornadoes, floods, or forest fires further increases the risk from environmental threats. The risk from human threat actors can be affected if key computing facilities are located in places that are difficult to secure or have high traffic, such as highways and areas with high crime rates.

2.2 Determine the Voice of the Organization

When assessed in the context of the Voice of the Environment, the Voice of the Organization supplies an understanding of the assets and services that must be defended. This helps the operational resilience practitioner to determine how they could be compromised. CERT-RMM process areas, specific goals, and specific practices provide a solid foundation for determining the Voice of the Organization. Many of these process areas begin with collecting, analyzing, and prioritizing information. This gives the operational resilience practitioner a fuller picture of defended assets and services and shows how those assets and services ensure the accomplishment of the organization's mission. This section provides a synopsis of relevant goals and practices within these process areas and their relevance to the IPOR. It breaks down the Voice of the Organization into two sub-voices: the Voice of the Mission and the Voice of the Service.

2.2.1 Determine the Voice of the Mission

The Voice of the Mission establishes the organizational context for the organization's operational resilience program. This program must first and foremost support the strategic objectives of the organization and provide value by increasing the resilience of the assets and services on which the organization relies. A successful operational resilience program, after all, enables the organization to accomplish its mission during times of stress. In today's tumultuous cybersecurity environment stress is, in many cases, the organization's natural state. CERT-RMM's Enterprise Focus process area provides a foundation for this step.

> *Enterprise Focus establishes the "critical few" for the organization – the high-value services that must be resilient to ensure mission achievement. This sets the focus for all operational risk-based activities in the organization. Through an enterprise focus, the direction and target for operational resilience management are established, operational risk management activities are coordinated, and actions are taken that enable the organization to perform adequately in achieving its targets* [Caralli & Allen 2010, Kindle location 6605].

2.2.1.1 Describe the Organization's Strategic Objectives and the Services that Support Them

Leadership communicates the organization's strategic objectives in various ways. Ideally, the organization will periodically complete a formal strategic planning process that results in a set of strategic objectives. However, given the speed at which many organizations move, the operational resilience practitioner may have to glean these strategic objectives through a variety of other sources. These sources include reports, feedback, and testimony to shareholders or congressional committees, as well as guidance provided by senior leadership through meetings, email, and verbally. It is important, however, to identify strategic objectives and achieve a consensus that their goals are clear, tangible, and achievable. These strategic objectives will determine the targets that organizational services must meet. As CERT-RMM points out, "Failure to keep assets and ser-

vices resilient may significantly impair the organization's ability to meet strategic objectives" [Caralli & Allen 2010, Kindle location 6629]. Additionally, the operational resilience practitioner must understand which factors are critical to successfully meeting the organization's strategic objectives. These factors provide indicators that help to bind the strategic and operational functions of the organization [Caralli & Allen 2010, Kindle locations 6655-6673]. The operational resilience practitioner can use them to identify services that enable the organization to achieve its strategic objectives. People, information, technology, facilities, and other assets support these services (i.e., business development, legislative services, or delivery of customer support such as health care, utilities, or consumer products).

2.2.1.2 Describe the Organizational Culture

Organizational culture is the set of beliefs, norms, and values that are commonly shared throughout an organization. The organizational culture is an important part of the Voice of the Organization for two reasons. First, a large percentage of attacks take advantage of the behavior of individuals with access to organizational assets and services. For instance, an attacker may exploit a lack of user awareness via social engineering, phishing, or spear phishing. Second, organizations face threats from those within the organization or who have access through an external dependency, such as a vendor. (External dependencies are discussed in greater detail in Section 2.2.2.2 below.)

The stated and enforced priorities of leadership and the effectiveness of organizational training and awareness programs have a large effect on whether the organizational culture can help or hinder a threat actor. For instance, if leadership has not emphasized that each member of the organization has an important role in maximizing operational resilience, its members will likely take a less active role. If organizational training and awareness fail to effectively motivate and inform members to do their part, they are likely to enhance the threat rather than diminish it.

On the other hand, motivated, trained, and aware members of an organization can add to its situational awareness. Individuals who are encouraged to look for and report suspicious activity in their computing environments and physical surroundings can act as sensors, diminishing a threat actor's ability to jeopardize or threaten organizational assets and services.

In addition, members of the organization may include threat actors. According to the *CERT Guide to Insider Threats*,

> *Insiders pose a substantial threat due to their knowledge of and access to their employers' systems and/or information. They bypass physical and electronic security measures through legitimate means every day. There is no demographic profile of a malicious insider—they are men and women, married and single, young and old, and cover a range of ethnicities* [Cappelli 2012, Kindle location 667].

The organization should identify factors in the Voice of the Environment that affect the intentions, capabilities, and prevailing attack patterns of insider threat actors. These factors include the organizational climate and the awareness of legal responsibilities and restraints like those discussed in Section 2.1.2 above. The *CERT Guide to Insider Threats* provides in-depth detail about three

categories of insider threats—insider IT sabotage, theft of IP, and insider fraud—and the characteristics that define them [Cappelli 2012, Kindle location 667].[7]

2.2.2 Determine the Voice of the Service

2.2.2.1 Describe Organizational Assets

To be successful, the high-value services identified in the Voice of the Mission must be supported by resilient assets (people, information, technology, and facilities). The organization must therefore identify these assets as specifically as possible. Large organizations may not be able to identify every asset that supports these services and must determine the level of specificity required. For instance, aggregating different asset types by subordinate organization may be sufficient to understand how a vulnerability that affects a specific asset could pose risks within a subordinate organization. However, organizations should try to be more specific about identifying assets that are more valuable and have a greater effect on high-value services. For instance, knowing the resilience of a data center that supports large numbers of organizational services might be worth the added detail. The Asset Definition and Management process area of CERT-RMM provides greater detail on this step [Caralli & Allen 2010, Kindle locations 2313-2557]. Understanding the organization's high-value assets enables the intelligence analyst and operational resilience practitioner to focus their efforts on identifying which intelligence needs are of greatest importance to the organization's risk profile. Analyzing the four categories of organizational assets—people, information, technology, and facilities—is discussed in greater detail in Appendix C.

2.2.2.2 Describe External Dependencies

CERT-RMM discusses specific goals and practices to identify and manage these dependencies in its External Dependencies Management (EXD) process area. According to EXD, "Regardless of the degree of external dependence, the organization retains responsibility for service mission assurance. The organization is responsible for setting the resilience requirements for services and related assets, communicating them to and requiring them of external entities, and monitoring to ensure external entities are meeting them."

In addition to identifying the external dependencies whose operational resilience is of interest to the organization, identifying those that provide a potential attack vector is also crucially important. Recent, highly publicized breaches exemplify compromised outside vendors with access to an organization's assets. Identifying these external dependencies helps intelligence collection and analysis providers to identify relevant intelligence. The External Dependencies Management (EDM) process area of CERT-RMM provides greater detail on this step [Caralli & Allen 2010, Kindle locations 7351-7548].

2.3 Determine the Voice of the Threat Actor

The three inputs to the IPOR—the Voice of the Environment, Voice of the Organization, and the Voice of the Threat Actor—are inextricably linked. As such, the Voice of the Threat Actor must be considered in the context of the environment that both the organization and the threat actor operate in, and the assets and services that the organization is trying to defend. A careful, objec-

[7] Additional information on insider threats can be found at http://www.cert.org/insider-threat/.

tive consideration of the Voice of the Environment and Voice of the Organization (as comprehensive as possible in the time allotted) combine to make the Voice of the Threat Actor more relevant to the organization's operational resilience program. The result of the Voice of the Threat Actor, and the IPOR as a whole, are a number of use cases for threat-actors (known as courses of action in IPB). These use cases feed into the organization's risk management process. Later, they become requirements for the organization's project management processes, which seek to mitigate the risks engendered by the threat actor use cases.

While a certain amount of generalization is necessary (no organization can be aware of each individual threat actor's intentions, capabilities, and past and potential attack patterns), applying historical data to the threat-actor category can provide important context to risk management.

2.3.1 Describe the Threat Actor

2.3.1.1 Develop Threat Actor Taxonomy

Because no organization knows every relevant threat actor, a degree of categorization is required to assess them. These categorizations must be clearly defined. In an interview during preparation of this report, Tim Casey of Intel Corporation noted that clear definitions are important because a single term such as "hacker" or "spy" has not only multiple understandings as to its ontology, but also multiple perceptions according to a hacker or spy's intentions, capabilities, and prevailing attack patterns. A comprehensive yet workable taxonomy of categorizations allows threat actors to be accounted for, which may not be utmost in the collective consciousness of the operational resilience community. Threats that are reported in the technical, trade, and traditional media often take precedence in this collective consciousness, which diverts attention from other sources of threats and risks to the organization [Casey 2007, p. 3].

In the Risk-Framing activity described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, organizations are advised to create a risk taxonomy that categorizes threat sources into three categories:

1. hostile cyber/physical attacks
2. human errors of omission or commission
3. natural and man-made disasters

NIST SP 800-39 goes on to say, "For threats due to hostile cyber-attacks or physical attacks, organizations provide a succinct characterization of the types of tactics, techniques, and procedures employed by adversaries that are to be addressed by safeguards and countermeasures" [NIST 2011, p. 35].

Intel Corporation's Threat Agent Library (TAL) is an example of such a taxonomy. In the TAL, Intel identifies 22 threat actor categories or "agents." Intel notes that an environmental threat category (such as natural and man-made disasters) can be added to the threat actor taxonomy, as annotated by NIST SP 800-39 [Casey 2007, p. 5]. The TAL then identifies eight "agent parameters" with possible parameter values:

- access (e.g., internal, external)
- outcome (up to two, e.g., acquisition/threat, business advantage, damage, embarrassment, technical advantage)

- limits on agent activities (maximum, e.g., code of conduct, legal, extra-legal minor, extra-legal major)
- resources (maximum, e.g., individual, club, contest, team, organization, government)
- skills (maximum, e.g., none, minimal, operational, adept)
- objective (one or more, e.g., copy, deny, destroy, damage, take, all of the above/don't care)
- visibility (minimum, e.g., overt, covert, clandestine, multiple/don't care) [Casey 2007, pp. 5-8].
- motivation (multiple,[8] e.g., accidental, disgruntlement, unpredictable, personal financial gain, organizational gain, personal satisfaction, notoriety, ideology, dominance) [Casey 2015, pp 2-8]

During our interview, Casey said that starting with a standardized taxonomy vastly improves the efficiency of risk management by eliminating many of the descriptive tasks associated with defining every category of threat. The ensuing analysis of historical data is more consistent because the data can be categorized according the domains associated with the taxonomy. The TAL is provided as an example of a threat-actor taxonomy. Operational resilience practitioners should research all available taxonomies and define a taxonomy that works for their organization. In fact, the categories in the TAL itself should be customized to the needs of the organization. The operational resilience practitioner should also consider the benefits of using a standardized taxonomy that facilitates sharing information across other operational resilience programs in industry and government.

2.3.1.2 Gather, Categorize, and Analyze Historical Threat Actor Data

Much of the unclassified information regarding threat actors, their prevailing attack patterns, and their preferred targets is currently locked up in incident reports, court records [Glenny 2012, Kindle location 4230], books, news stories, and database entries. Threat actors themselves can be an excellent source of information, either through anonymous chat forums or through direct interaction [Glenny 2012, Kindle location 4244]. Techniques such as text analysis and machine learning can derive patterns that reveal both the prevailing attack patterns of threat groups and their preferred target types.

Using these data sources to identify trends in the intentions, capabilities, and attack patterns of threat actors is very similar to developing performance metrics within an organization. The process is called Goal, Question, Indicator, Metric (GQIM) [Stewart et al 2015, p. 11]

1. Develop threat actor goal statements that are relevant to the organization, based on outcomes from Voice of the Environment and Voice of the Organization. For instance, were we to use Intel's TAL, we could combine one or more agents (e.g., anarchist, civil activist, and sensationalist) with a combination of agent parameters (e.g., access, outcome, objective) and high-value services and/or assets. An example might be, "Threat actors such as anarchists, civil

[8] Intel Corp. breaks down motivation into defining and co-motivation. Co-motivation is broken down into subordinate, binding, and personal motivation. More information can be found in its whitepaper at http://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/understanding-cyberthreat-motivations-to-improve-defense-paper.html.

activists, and sensationalists would like to use external access to embarrass the organization by denying access to our e-commerce services."

2. Develop plain-English questions that elucidate whether the threat actor is likely to create an impact based on current data. An example might be, "What is the possibility that a threat actor may disrupt our access to our e-commerce capabilities being hosted in our cloud service provider (CSP)?"
3. Identify indicators, which are pieces of information necessary to create a metric to answer the question. An example might be, "Instances of known denial-of-service-attacks by date which denied organizational access to assets and services hosted by their CSP." Another might be, "Instances of mention of denial of service against CSP access in known hacker forums."
4. Develop a metric that proves or disproves a hypothesis, such as, "There is a correlation between mentioning denials of service in known hacker forums and instances of denials of service to CSPs."

The division of responsibilities between intelligence provider and operational resilience practitioner is a result of the ongoing, collaborative relationship of trust first mentioned in Section 1.4.1 above. If the intelligence provider believes that knowledge of specific metric construction components could compromise his or her sources, the operational resilience practitioner should be the one who develops goal and question statements while the intelligence provider develops indicators and metrics. This is especially true if the intelligence resides on classified systems to which the operational resilience practitioner does not have access.

2.3.2 Develop Threat Use Cases

The combined details of threats should be documented in threat use cases. These use cases include categories of threat actors, what they hope to achieve, their motivations for doing so, the organizational assets and services threatened, and the most likely way they will create the threat. Although this set of threat use cases may grow large, building out a larger set for later prioritization through risk management is important. Each threat use case should be as detailed as time and resources allow. Each threat use case should include a set of indicators and collection requirements to enable the organization to continue monitoring the likelihood and potential impact of the threat.

The threat use case then becomes the input for the risk management framework in use by the organization. In the next section, we describe how CERT-RMM, OCTAVE, and the NIST RMF can be used to prioritize these threats into a risk-management approach.

3 Integration with Management Frameworks

To make use of intelligence, the operational resilience practitioner does not need to create a competing process independent of other organizational frameworks. In fact, using intelligence products to manage operational resilience is not only compatible with many existing frameworks but is frequently inherent. This section provides an overview of how to operationalize intelligence products in order to build operational resilience of organizational assets and services. As discussed in the previous section, the threat use case becomes a unit of work for each risk-management framework.

3.1 Application to Resilience and Risk Management Frameworks

3.1.1 CERT Resilience Management Model (CERT-RMM)

CERT-RMM is a capability model for managing and improving operational resilience. The model's goals and practices are grouped into 26 process areas. Organizations that use CERT-RMM can use the results of the intelligence process to satisfy four goals in two process areas to improve operational resilience.

When performing functions as part of the Vulnerability Analysis and Resolution (VAR) process area, the specific practice Analyze Vulnerabilities (VAR:SG2:SP3) requires "understanding the threat and exposure" of the vulnerability [Caralli & Allen 2010, Kindle location 20889]. To perform this analysis, the operational resilience practitioner must have up-to-date, consumable information. More holistic, precise intelligence enables the organization to more accurately analyze its vulnerabilities and identify the threats and risks that they engender.

The Risk Management (RISK) process area enables agencies to "identify analyze, and mitigate risks to organizational assets that could adversely affect the operation and delivery of services" [Caralli & Allen 2010, Kindle location 16089]. CERT-RMM defines operational risk as "the potential impact on assets and their related services that could result from inadequate or failed internal processes, failures of systems or technology, the deliberate or inadvertent actions of people, or external events" [Caralli & Allen 2010, Kindle location 21941]. The output of the VAR process and the underlying intelligence are critical to successfully managing risk. An effective intelligence process enables the operational resilience practitioner to

- determine risk sources and categories (RISK:SG1:SP1)
- identify risk (RISK:SG3)
- evaluate risk (RISK:SG4)

Continuously reassessing and reevaluating the Voice of the Threat Actor, Voice of the Environment, and Voice of the Organization ensures that the facts and assumptions underpinning risk analysis remain timely and relevant. Institutionalizing the intelligence-preparation process by performing generic practices (such as establishing a governance process (RISK:GG2:GP1), planning the intelligence preparation process (RISK:GG2:GP2), and providing dedicated resources to the analysis and use of intelligence products (RISK:GG2:GP3)) as part of a risk management program enables organizations to develop a mature program that is more effective, repeatable, and respon-

sive to stress [Caralli & Allen 2010, Kindle locations 16125-25982]. Maturing the interaction with intelligence sources aids in this institutionalization.

3.1.2 Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro Methodology

OCTAVE Allegro contains activities, steps, worksheets, and questionnaires that formally capture many elements of the Voice of the Organization, Voice of the Environment, and Voice of the Threat Actor. A worksheet that enables the capture of information gleaned through intelligence analysis is the Information Asset Risk Worksheet. This form enables the organization to identify

- the information asset
- area of concern
- threat actor
- means
- motive
- outcome
- security requirements
- probability
- consequences
- risk mitigation

Use of OCTAVE Allegro in a robust cyber intelligence program could create a continuous cycle of understanding defended assets and services as well as the threat environment which exposes those assets and services to operational risk.

3.1.3 National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)

The NIST RMF is a framework described in NIST Special Publication (SP) 800-37 for federal systems. The framework consists of the following steps [NIST 2010, pp. 7-8]:

1. Categorize the information system and the information that it processes, stores, and transmits based on an impact analysis.
2. Select an initial set of baseline security controls for the information system based on the security categorization.
3. Tailor and supplement the security control baseline as needed based on an organizational assessment of risk and local conditions.
4. Implement the security controls. Describe how the controls are employed within the information system and its environment of operation.
5. Assess the security controls using appropriate assessment procedures. Determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

6. Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the nation resulting from the operation of the information system and the decision that this risk is acceptable.

A common fallacy is that an organization must select and apply only the controls designated for the impact level of their system exactly as they are prescribed in NIST SP 800-53. The truth is that these controls represent the minimum baseline. The NIST RMF also discusses tailoring controls "if necessary, with additional controls and/or control enhancements to address unique organizational needs based on…specific threat information" [NIST 2010, p. 25]. The framework is, after all, a risk-management framework, not merely a controls-management framework. Task 5-3 of the NIST RMF recommends that organizations employ formal or informal risk assessments "at the discretion of the organization to provide needed information on threats, vulnerabilities, and potential impacts as well as the analyses for the risk mitigation recommendations." [NIST 2010, p. 35]. This cycle of assessing risks and tailoring controls carries an up-front investment of time. But it would pay long-term dividends if a potential incident was avoided.

3.2 Application to Project Management Frameworks

Once the risk management process has been initiated based on threat intelligence, use common project management methodologies to directly manage mitigations. This section provides a brief discussion of how to operationalize intelligence products in order to support effective project management.

3.2.1 Agile

Agile is based on the Plan-Do-Check-Act cycle and emphasizes continuous delivery of functionality. Functionality is delivered in sprints of approximately one to four weeks. During the planning phase, requirements are documented in user stories that are then identified from the project backlog for inclusion in the next sprint. By coupling intelligence with an effective risk management program (such as one based on CERT-RMM's RISK process area or the NIST RMF), mitigation strategies can be operationalized in short bursts. A continuous process of intelligence analysis, coupled with the short-time-cycle nature of the Agile methodology, enables risk management to evolve and adapt to changes in threat intelligence but still be implemented in a controlled, deliberate fashion.

3.2.2 Project Management Body of Knowledge (PMBOK)

The Project Management Institute's PMBOK consists of six project management process groups and 10 knowledge areas. When initiating a project that supports the organization's operational resilience, one of the inputs to Process 4.1, "Develop Project Charter," is the business case [PMI 2013, Kindle location 1930]. When initiating a project that will improve the operational resilience of organizational assets and services, a robust intelligence program can help to develop an impactful, descriptive business case. Process 5.2 describes the collection of requirements for the project [PMI 2013, Kindle location 26828]. For system projects, this can include identifying quality attributes for the system's architecture based on stakeholder requirements, such as performance, reliability, and modifiability [Clements 2011, Kindle locations 767, 789-801]. A robust intelligence process (as discussed regarding the planning phase of Agile) also supports this process in PMBOK. A requirements traceability matrix shows connections between requirements and the

intelligence products that support them. Additionally, it makes re-evaluating requirements easier, ensuring that the underlying threat information is still valid. An intelligence-supported risk management problem statement also facilitates scope definition in Process 5.1 [PMI 2013, Kindle location 2593] by prioritizing operational resilience requirements and ensuring the most pressing risks are addressed and decisions to accept risks are based on a sound logical foundation.

4 Conclusion

Operational resilience practitioners require a method to methodically inject threat-actor intelligence into their resilience, risk, and project-management methodologies. IPOR proposes a framework to enable operational resilience practitioners to develop a relationship with their intelligence provider, identify their intelligence needs, consume that intelligence, integrate it into their risk-management processes, and then mitigate those risks through effective project management. The U.S. military has a long history of integrating intelligence collection and analysis into mission analysis and planning functions through the MDMP and IPB processes. IPOR builds upon IPB to develop a model that is accessible by operational resilience practitioners in a wide variety of environments. By using and further developing IPOR, operational resilience practitioners take part in an end-to-end process that enables a structured consideration of the Voice of the Environment, Voice of the Organization, and Voice of the Threat Actor in their resilience, risk, and project management functions.

Appendix A. Using Behavioral Models to Customize Information for Executive and Middle Management Audiences

An organization rarely makes decisions as a monolithic rational actor with a unified set of intents and desired outcomes. Graham Allison and Philip Zelikow termed this the Rational Actor model of government decision making in their book, *Essence of Decision: Explaining the Cuban Missile Crisis* [Allison & Zelikow 1999, Kindle location 508]. Developing a common situational awareness and a coordinated approach to acting upon that awareness requires more nuanced models of thought. They enable those who collect data, analyze it, and make decisions about it to do so with a more effective understanding of those who impact the process and those who are affected by it.

One example is the Organizational Behavior model. Through this model, organizational actions (in the case of the Cuban Missile Crisis, those of governments) are viewed as outputs that are shaped by existing strategies, processes and procedures [Allison & Zelikow 1999, Kindle location 3235].

> *To perform complex tasks, the behavior of large numbers of individuals must be coordinated. Coordination requires standard operating procedures: rules according to which things are done. Reliable performance of action that depends upon the behavior of hundreds of persons requires established "programs"…* [Allison & Zelikow 1999, Kindle location 3240]

> *The behavior of these organizations—and consequently of the government—relevant to an issue in any particular instance is, therefore, determined primarily by routines established prior to that instance. Explanation of a government action starts from this baseline, noting incremental deviations. But organizations do change. Learning occurs gradually, over time* [Allison & Zelikow 1999, Kindle location 3246]

An organization can make faster and more effective decisions about resiliency by developing intelligence requirements that adjust to changes in the environment and take existing procedures, practices, and capabilities into account. In turn, these decisions can be executed more effectively and can lead to the perpetuation of faster, more effective follow-on OODA Loops.

Effective intelligence products derive greater impact through tailoring to executive stakeholders. This is done through a model that Graham and Zelikow called the Governmental Politics model.

> *Both by charter and in practice, most players "represent" a department or agency along with the interests and constituencies their organization services. Because their preferences and beliefs are related to the different organizations they represent, their analyses yield conflicting recommendations. Separate responsibilities laid on the shoulders of distinct individuals encourage differences in what each sees and judges to be important* [Allison & Zelikow 1999, Kindle location 5603].

"Politics" in this regard does not indicate a self-serving nature, but rather the differences in viewpoint that each decision maker's mission engenders. These differences mean that those who develop resilience-related products must understand these unique mission-related viewpoints and

tailor outputs accordingly. Through data science and visualization, resilience practitioners can deliver the intelligence products necessary for decision makers to perform according to their most relevant considerations.

Appendix B. Common Psychological Distortions in Intelligence Analysis

Although this report seeks to avoid in-depth discussion of intelligence collection and analysis practices, it is important to understand the pitfalls inherent in intelligence analysis. As stated in Section 1.4.5., the operational resilience practitioner must analyze the analysis. Therefore, he or she must be aware of common psychological pitfalls that typically befall the process. In *The Psychology of Intelligence Analysis*, Richards Heuer identified 12 biases that can affect how intelligence is perceived:

1. Vividness. “Information that is vivid, concrete, and personal has a greater impact on our thinking than pallid, abstract information that may actually have substantially greater value as evidence” [Heuer 1999, p. 116].
2. Absence of Evidence. Hypotheses for which there is little or no evidence are discounted, giving those for which evidence exists outsized consideration [Heuer 1999, p. 119].
3. Oversensitivity to Consistency. “The internal consistency in a pattern of evidence helps determine our confidence in judgments based on that evidence” [Heuer 1999, p. 120]. That is, the more we see coherent patterns in the information, the more we are likely to perceive it as accurate.
4. Uncertain Accuracy. “In processing information of uncertain accuracy or reliability, analysts tend to make a simple yes or no decision. If they reject the evidence, they tend to reject it fully, so it plays no further role in their mental calculations. If they accept the evidence, they tend to accept it wholly, ignoring the probabilistic nature of the accuracy or reliability judgment” [Heuer 1999, p. 122].
5. Persistence of Impressions Based on Discredited Evidence. “Impressions tend to persist even after the evidence that created those impressions has been fully discredited” [Heuer 1999, p. 124].
6. Bias In Favor of Causal Explanations. “People expect patterned events to look patterned, and random events to look random, but this is not the case. Random events often look patterned” [Heuer 1999, p. 130].
7. Bias Favoring Perception of Centralized Direction. “Very similar to the bias toward causal explanations is a tendency to see the actions of other governments (or groups of any type) as the intentional result of centralized direction and planning” [Heuer 1999, p. 131]. This is comparable to Allison and Zelikow’s Rational Actor Model discussed in Section 1.4.4 above.
8. Similarity of Cause and Effect. “Analysts tend to assume that economic events have primarily economic causes, that big events have important consequences, and that little events cannot affect the course of history. Such correspondence between cause and effect makes a more logical and persuasive—a more coherent—narrative, but there is little basis for expecting such inferences to correspond to historical fact” [Heuer 1999, p. 133]. An example is a minor computer glitch that affects the operations of a stock exchange, causing billions of dollars of losses.

9. Internal vs. External Causes of Behavior. “A fundamental error made in judging the causes of behavior is to overestimate the role of internal factors and underestimate the role of external factors” [Heuer 1999, p. 134].
10. Overestimating Our Own Importance. “Individuals and governments tend to overestimate the extent to which they successfully influence the behavior of others” [Heuer 1999, p. 138]. For instance, a nation may assume that its actions directly cause another nation’s actions, when in fact they are caused by a third nation’s actions.
11. Illusory Correlation. “Correlation alone does not necessarily imply causation. For example, two events might co-occur because they have a common cause, rather than because one causes the other” [Heuer 1999, p. 140].
12. Denial and Deception. Evidence often leads to a hypothesis as a result of denial and deception on the part of the threat actor [Heuer 1999, p. 98]. For instance, a threat actor may use a denial-of-service attack to cloak the fact that the core of the attack is actually a data exfiltration exploit.

Understanding one’s own psychology when assessing intelligence makes it easier to spot inconsistencies or omitted information and allows the resilience practitioner to recognize when he or she is not perceiving intelligence accurately.

Appendix C. Describing Organizational Assets

When defining organization assets (as discussed in Section 2.2.2.1 above), it is normally helpful to consider all four categories of organizational assets: people information, information, technology, and facilities. Once defined, these assets must be reviewed as they will likely change over time. The following paragraphs describe the differences between the four categories and how they can be considered when performing IPOR.

C.1 Describe People Assets

Identify and describe the roles of staff members whose operational resilience is of high value to the organization. They could include individuals with higher-level security clearances, executives, and staff with high visibility to the public. These key personnel are not simply the targets of attacks; if their identities are compromised, threat actors could launch additional attacks upon the organization. For example, an email sent from the compromised account of an executive is likely to face a lower level of scrutiny from recipients within the organization. The recipients of such email would be more likely to click an unsafe link, open an unsafe attachment, or perform other unsafe actions. If an organization can spot a prevailing attack pattern through intelligence collection and analysis, it can proactively mitigate these threats. For example, it could require all executives to digitally sign their outgoing emails.

Personnel involved in business continuity/disaster relief (BC/DR) should also be identified and their current disposition noted (e.g., the person is on vacation or the position is vacant). For example, an incoming hurricane would pose a higher risk if the organization's lead for BC/DR were to be unavailable during that time. The People Management process area of CERT-RMM provides greater detail on this step [Caralli & Allen 2010, Kindle locations 15373-15502].

C.2 Describe Information Assets

Identify and describe the organization's high-value information assets. According to CERT-RMM, "An information asset can be described as information or data that is of value to the organization, including such diverse information as patient records, intellectual property, vital business, records, vital business records and contracts, and customer information." By tying these information assets to high-value services, the organization can better assess the willingness of a threat actor to access, destroy, or manipulate the data. It also can prioritize intelligence about threats against these information assets. Categorizing this data into various levels of sensitivity and their relationship to specific security requirements (such as those established by the statutes mentioned in Section 2.1.2 above), enables intelligence providers to focus on the information that is most relevant. The Knowledge and Information Management process area of CERT-RMM provides greater detail on this step [Caralli & Allen 2010, Kindle locations 11410-11509].

C.3 Describe Technology Assets

The types and existence of technologies define the types of attack vectors and the attack patterns that rely on them. When organizations inventory their networks, they often find that outdated and unsupported technologies are vital to supporting high-value services. Understanding the organiza-

tion's technological surface area is critical to understanding the capabilities and prevailing attack patterns of threat actors. Knowing the organization's hardware and software assets is vital. According to CERT-RMM, in addition to the relationship between the technology and service, the following criteria may be used to establish high-priority technological assets:

- the relationship between the technology and the value of the information assets stored, transported, or processed by the technology
- technology assets such as networks that are considered to be foundational and are vital to supporting more than one organizational service
- proprietary technology assets provided by suppliers (such as application systems or specific types of hardware) that would materially affect the organization if the supplier is unreachable or drops support [Caralli & Allen 2010, Kindle locations 19668-19677].

After high-priority technological assets are identified (if only categorically), intelligence professionals can seek out trends and relevant events of key planning importance to the operational resilience practitioner. The Technology Management process area of CERT-RMM provides greater detail on this step [Caralli & Allen 2010, Kindle locations 19617-19723].

C.4 Describe Facility Assets

Threats and risks to facilities have an outsized effect on the risk profile of the organization. According to CERT-RMM, the following criteria can be used to establish high-priority facilities:

- the use of the facility asset in the general management and control of the organization (corporate headquarters, primary data centers, etc.)
- facility assets that are important to supporting more than one service
- the value of the asset in directly supporting the organization's achievement of critical success factors and strategic objectives
- the organization's tolerance for pain—that is, the degree to which it can suffer a loss or destruction of a facility asset and still meet its mission [Caralli & Allen 2010, Kindle locations 5802-5812].

After the high-priority facilities are identified (if only categorically), the intelligence professional can seek out trends and relevant events of key planning importance to the operational resilience practitioner. If threat actors have penetrated the defenses of similar facilities, or natural threat actors such as floods have compromised the resilience of similar facilities, intelligence collection and analysis can better spot information of importance to the organization. The Environmental Control process area of CERT-RMM provides greater detail on this step [Caralli & Allen 2010, 5756-5847].

Appendix D. Comparison of IPB and IPOR

Although IPB is the starting point for developing IPOR, IPB steps and sub-steps do not always directly correspond to IPOR voices and sub-steps. Table 1 provides a reference for those familiar with the IPB process for how IPOR captured and built on these considerations.

Table 1: Comparison of IPB and IPOR

IPB Step[9]	IPB Sub Step	IPOR Voice	IPOR Sub Step
Define the Operational Environment	Identify the limits of the commander's area of operations	Voice of the Organization	Determine the Voice of the Mission
Define the Operational Environment	Identify the limits of the commander's area of interest	Voice of the Environment	All
Define the Operational Environment	Identify significant characteristics of the areas of operations and areas of interest for further analysis	Voice of the Environment	All
Define the Operational Environment	Initiate process necessary to acquire information necessary to complete IPB	Voice of the Environment Voice of the Organization Voice of the Threat	All
Describe Environmental Effects on Operations	Describe how the operational environment influences friendly and threat COAs	Voice of the Environment	All
Describe Environmental Effects on Operations	So what? - Identify how relevant characteristics of the area of interest will affect friendly and threat operations	Voice of the Environment	All
Evaluate the Threat	Evaluate the threat	Voice of the Threat	Describe the Threat Actor
Evaluate the Threat	Identify threat characteristics	Voice of the Threat	Describe the Threat Actor
Determine Threat Courses of Action	Develop threat COAs	Voice of the Threat	Determine Threat Use Cases
Determine Threat Courses of Action	Develop event template and matrix	Voice of the Threat	Determine Threat Use Cases

[9] Army Techniques Publication 2-01.3 provides the background and process for IPB and can be accessed by the public at http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/atp2_01x3.pdf

Appendix E. Acronym List

Acronym	Definition
CERT-RMM	CERT Resilience Management Model
CSP	Cloud Service Provider
IPB	Intelligence Preparation of the Battlefield
IPOR	Intelligence Preparation for Operational Resilience
IPECC	Initiating, Planning, Executing, Executing, Monitoring and Controlling, Closing
MDMP	Military Decision-Making Process
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OODA	Observe, Orient, Decide, Act
PA	Process Area
PDCA	Plan, Do, Check, Act
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
RMF	Risk Management Framework
SG	Specific Goal
SP	Special Publication (NIST) or Specific Practice (CERT-RMM)
TAL	Threat Agent Library

References

URLs are valid as of the publication date of this document.

[Allison & Zelikow 1999]

Allison, G. T. & Zelikow, P. *Essence of Decision: Explaining the Cuban Missile Crisis* 2nd ed. (Kindle Edition, location 3235). Longman. 1999.

[Barnum & Sethi 2007]

Barnum S. & Sethi, A. *Attack Patterns as a Knowledge Resource for Building Secure Software.* Cigital, Inc. 2007.

[Boyd 1996]

Boyd, John R. *The Essence of Winning and Losing*. 1996. https://fasttransients.files.wordpress.com/2010/03/essence_of_winning_losing.pdf

[Capelli et al 2012]

Cappelli et al. *The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).* Addison-Wesley. 2012.

[Caralli & Allen 2010]

Caralli, R. & Allen, J. *The CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley. 2010.

[Casey 2007]

Casey, T. *Threat Agent Library Helps Identify Information Security Risks*. Intel Corporation. 2007. https://communities.intel.com/docs/DOC-1151.

[Casey 2015]

Casey, T. *Understanding Cyberthreat Motivations to Improve Defense.* Intel Corporation. 2015. http://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/understanding-cyberthreat-motivations-to-improve-defense-paper.html

[Clements 2011]

Clements, P. *Documenting Software Architectures: Views and Beyond* (2nd ed.) (Kindle version). Addison-Wesley. 2011.

[Covey 2013]

Covey, S. R. *The 7 Habits of Highly Effective People* (Kindle Edition). Simon & Schuster. 2013.

[Endsley 2012]

Endsley, M. & Jones, D. *Designing for Situation Awareness: An Approach to User-Centered Design* (2nd ed.). CRC Press. 2012.

[Glenny 2012]

Glenny, M. *Darkmarket: How Hackers Became the New Mafia* (Kindle Edition). Vintage Books. 2012.

[Gray 2015]

Gray, D. Leveraging Threat Intelligence to Support Resilience, Risk, and Project Management [blog post]. *SEI Blog*. September 28, 2015. https://insights.sei.cmu.edu/sei_blog/2015/09/leveraging-threat-intelligence-to-support-resilience-risk-and-project-management.html

[Heuer 1999]

Heuer, R. *Psychology of Intelligence Analysis.* Center for the Study of Intelligence, Central Intelligence Agency. 1999.

[NIST 2010]

NIST SP 800-37. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Life Cycle Approach*. Department of Commerce (NIST). 2010.

[NIST 2011]

NIST SP 800-39. *Managing Information Security Risk: Organization, Mission, and Information System View*. Department of Commerce (NIST). 2011.

[PMI 2013]

A Guide to the Project Management Body of Knowledge (PMBOK® Guide). Project Management Institute (PMI). 2013.

[Rustad 2009]

Rustad, M. *Internet Law in a Nutshell*. West Academic Publishing. 2009.

[Stewart et al. 2015]

Stewart, K. et al. *Measuring What Matters Workshop Report* (CMU/SEI-2015-TN-002). Software Engineering Institute, Carnegie Mellon University, 2015. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=433515

[U.S. Army 2012]

ADP 5-0. *The Operations Process*. Department of the Army. 2012.

[U.S. Army 2014]

ATP 2-01.3. *Intelligence Preparation of the Battlefield*. Department of the Army. 2014.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	Month and Year (date added at time of publication)	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Intelligence Preparation for Operational Resilience (IPOR)	FA8721-05-C-0003

6. AUTHOR(S)

Douglas Gray

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2015-SR-033

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Distribution Statement A: Approved for Public Release; Distribution is Unlimited	

13. ABSTRACT (MAXIMUM 200 WORDS)

Operational resilience practitioners in industry, government, and the military have the unenviable task of recommending and acting upon priorities to enable their organizations to accomplish their missions during times of stress. However, for many, a formal method of acquiring and leveraging objective threat intelligence to support resilience, risk, and project management has remained elusive. This special report proposes a framework called Intelligence Preparation for Operational Resilience (IPOR) to create a model for structured analysis of their intelligence needs and a way to operationalize threat intelligence once they have received it. The IPOR references and builds upon frameworks such as the military's Intelligence Preparation of the Battlefield process and the CERT® Resilience Management Model to build a structure to meet this end.

14. SUBJECT TERMS	15. NUMBER OF PAGES
operational resiliency, threat actor, IPOR, intelligence	41

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102